Remarks

The Examiner has required that Applicant provide certain information pursuant to 37 C.F.R. §1.105.

In particular, the Examiner has asked the Applicant to:

1. Identify GP_sec AH and EPsec_AH as used in the claims.
2. Identify HMAC as used in the claims.
3. Identify whether the authentication key is a public or private key.

In response to the request, Applicant has amended the claims of the application to replace the language of GPsec_AH and EPsec_AH with 'IPsec_AH', as the terms 'GPsec_AH and EPsec_AH were spelling errors that had inadvertently been included in the claims. The Examiner is thanked for the thorough review of the claims.

With regard to the request to identify HMAC, HMAC is a term that is well known in the art to mean a mechanism for message authentication using cryptographic hash functions. The HMAC mechanism is described in Internet Engineering Task Force (IETF) Request for Comments (RFC) 2104, which Applicants have included in an Information Disclosure Statement filed herewith. In addition, Applicant has also filed as part of an IDS definitions of the terms 'MD5' and 'SHA-1', which are also terms of the art.

Applicant submits that the submissions overcome the inadequacies of the specification.

With regard to the issue of whether the authentication key is a private or public key, Applicants note that the specification clearly states at page 9, lines 2-3 that 'the authentication key 308 is a symmetric encryption key that is used to authenticate the host and establish a security agreement between the host and the DR...' At page 9 the specification also clearly states:

'the key server 118 distributes a special encryption key ... to all routers in the all routers group, for example using public key encryption, and uses the router key to encrypt access information. The encrypted access information is then distributed to the all routers in the

group. The multicast routers in the all routers group use the router key to decrypt the access information..."

At page 10, lines 1-3, the specification states:

'Thus, when the host requests a group key from the key server 118, the key server 118 authenticates the host, generates access information for the host, and sends access information to both the host and the DR...'

The authentication key is part of the access information that is forwarded to the host and the DR, to provide a symmetric key as described in the specification. The access information may be encrypted using the router key.

Applicants would submit that this information, in particular the indication that they key is a symmetric key, would be sufficient to allow the Examiner to review the case, as it clearly describes 'the manner of distribution' of the keys, which appears to be the question at issue for the Examiner.

Conclusion

Applicants have made a diligent effort to respond to the request for information. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Lindsay G. McGuinness, Applicants' Attorney at 978-264-6664 so that such issues may be resolved as expeditiously as possible.

Respectfully Submitted,

12/4/2006
Date

_/Lindsay mcGuinness/_____
Lindsay G. McGuinness, Reg. No. 38,549
Attorney/Agent for Applicant(s)
McGuinness & Manaras LLP
125 Nagog Park Drive
Acton, MA 01720
(978) 264-6664

Docket No. 120-147